FUNDAÇÃO OSWALDO ARANHA
CENTRO UNIVERSITÁRIO DE VOLTA REDONDA
CURSO DE GRADUAÇÃO EM DIREITO
TRABALHO DE CONCLUSÃO DE CURSO

JÉSSICA BADARÓ E SILVA

CRIMES CIBERNÉTICOS E A LEGISLAÇÃO BRASILEIRA

VOLTA REDONDA
2023

FUNDAÇÃO OSWALDO ARANHA
CENTRO UNIVERSITÁRIO DE VOLTA REDONDA
CURSO DE GRADUAÇÃO EM DIREITO
TRABALHO DE CONCLUSÃO DE CURSO

CRIMES CIBERNÉTICOS E A LEGISLAÇÃO BRASILEIRA

Monografia apresentada ao Curso de Direito do UniFOA como requisito à obtenção do título de bacharel em Direito.

Aluna:
Jéssica Badaró e Silva

Professora Orientadora:
Éricka Júlio Batitucci

VOLTA REDONDA
2023

Fundação Oswaldo Aranha

UniFOA

FOLHA DE APROVAÇÃO

Trabalho de Conclusão de Curso intitulado:

CRIMES CIBERNÉTICOS E A LEGISLAÇÃO BRASILEIRA

Elaborado por Jéssica Badaró e Silva, apresentado publicamente perante a Banca Avaliadora como parte dos requisitos para conclusão do Curso de Direito.

Aprovado em 20 de junho de 2023

Banca Avaliadora:

.....

Professor(a) Orientador(a) - Unifoa

.....

Professor(a) Avaliador(a) - Unifoa

.....

Professor(a) Avaliador(a) - Unifoa

Aos meus pais.

AGRADECIMENTOS

Agradeço a Deus por ter me dado disposição e saúde durante os anos de graduação.

À minha orientadora pelas sugestões e pelo auxílio durante a elaboração deste trabalho.

À minha família, em especial meus pais, pelo suporte e incentivo.

RESUMO

A monografia tem por objetivo analisar como a legislação brasileira pode auxiliar na prevenção de ataques cibernéticos a empresas e a pessoas físicas. Para isso, buscou-se visualizar quais são as principais normas que dispõe sobre o ambiente virtual no Brasil, indicar os impactos dos crimes cibernéticos na sociedade, demonstrar como a Lei Geral de Proteção de Dados Pessoais pode auxiliar na proteção de dados dos clientes nas empresas e apontar as consequências do vazamento de dados nas empresas. A metodologia utilizada foi a pesquisa através de materiais bibliográficos, sites, notícias, jurisprudência, artigos e dados estatísticos. Portanto, a partir do presente trabalho foi possível observar que os dispositivos normativos que punem os sujeitos ativos dos crimes cibernéticos (Lei Carolina Dieckmann, Lei nº 14.155/2021 e Código Penal), a definição dos parâmetros para o uso da Internet no Brasil (Marco Civil da Internet) e as sanções administrativas para o descumprimento da LGPD podem auxiliar na prevenção dessa modalidade de crime cada vez mais frequente na era da informação.

Palavras-chave crimes cibernéticos; legislação brasileira; vazamento de dados.

SUMÁRIO

1 INTRODUÇÃO 8

2 ERA DA INFORMAÇÃO 9

3 DIREITOS FUNDAMENTAIS 13

3.1 Proteção dos dados pessoais.....14

3.2 Privacidade.....15

3.3 Liberdade de expressão 15

3.4 Sigilo da correspondência, da comunicação e dos dados.....15

4 LEGISLAÇÃO BRASILEIRA.....17

4.1 Marco Civil da Internet.....18

4.2 Lei Carolina Dieckmann.....20

4.3 Lei nº 14.155/2021.....21

5 CONVENÇÃO DE BUDAPESTE.....24

6 CRIMES CIBERNÉTICOS 26

6.1 Principais crimes cibernéticos.....28

6.2 Classificação.....29

6.3 Sujeito ativo e sujeito passivo.....30

6.4 Métodos.....31

7 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS 33

7.1 As empresas e a LGPD.....34

7.2 Consequências.....35

7.3 Jurisprudência.....37

8 ATAQUES CIBERNÉTICOS A EMPRESAS.....41

9 CONSIDERAÇÕES FINAIS.....44

10 REFERÊNCIAS.....45

1 INTRODUÇÃO

A justificativa dessa pesquisa é o aumento do número de casos de crimes virtuais e do vazamento de dados através de ataques cibernéticos no Brasil e no mundo. O Brasil é o 5º maior alvo de crimes cibernéticos, ficando somente atrás dos EUA, Reino Unido, Alemanha e África do Sul (ÉPOCA NEGÓCIOS, 2021). Essas modalidades de delito têm gerado prejuízos para pessoas físicas, pessoas jurídicas e países. Com a popularização do ambiente virtual, criminosos têm estabelecido diversas técnicas para atingir potenciais vítimas.

O objetivo geral do presente trabalho é analisar como a legislação brasileira pode auxiliar na prevenção de ataques cibernéticos a empresas e a pessoas físicas. Para o alcance desse objetivo, a metodologia utilizada foi a pesquisa através de materiais bibliográficos, sites, notícias, jurisprudência, artigos e dados estatísticos.

Os objetivos específicos são a) visualizar quais são as principais normas que dispõe sobre o ambiente virtual no Brasil, b) indicar os impactos dos crimes cibernéticos na sociedade, c) demonstrar como a Lei Geral de Proteção de Dados Pessoais pode auxiliar na proteção de dados dos clientes nas empresas e d) apontar as consequências do vazamento de dados nas empresas.

No primeiro capítulo, são feitas considerações sobre a sociedade atual e as principais transformações ao longo do tempo que possibilitaram esse contexto. No segundo capítulo, são elencados os direitos fundamentais que se inserem na era da informação. O terceiro e quarto capítulo abrangem as principais leis e um tratado internacional que dispõe sobre o ambiente virtual.

O quinto capítulo discorre sobre os principais crimes cibernéticos, a classificação, o sujeito ativo e passivo e os métodos utilizados por criminosos para a prática dessas infrações. O sexto capítulo trata sobre melhores práticas em proteção de dados, as consequências para as empresas em caso de descumprimento da Lei nº 13.709/2018 e jurisprudências sobre a LGPD. No último capítulo, são pontuados alguns tipos de ataques cibernéticos a empresas.

2 ERA DA INFORMAÇÃO

Com o advento de dispositivos informáticos como smartphones, tablets e computadores foi possível que ocorresse uma profunda transformação na forma como as pessoas se comunicam, transmitem e recebem informações. Além disso, a internet também permitiu que as informações pudessem se propagar entre curtas e grandes distâncias de modo instantâneo.

Essas modificações possibilitadas pelas tecnologias de informação e comunicação (TICs) e o acesso à internet permeiam várias áreas, como as de lazer, trabalho, saúde, educação, entre outras. Porém, essas tecnologias não são acessadas de modo igualitário em todo o mundo. Nos países em desenvolvimento e em regiões de infraestrutura limitada, são muitos os empecilhos para que as TICs sejam utilizadas em larga escala.

A sociedade da informação é, segundo Renato Martini (2017, p. 25), “infraestrutura da informação, tecnologia da informação”. Como demonstra Emerson Freire e Sueli Batista, a sociedade da informação foi iniciada na segunda metade do século XX e possui as seguintes características:

> Década de 70: início da informatização da sociedade nas principais cidades ocidentais desenvolvidas.
> Década de 80: início da popularização da internet.
> Década de 90: popularização do microcomputador.
> Início do século XXI: desenvolvimento da computação sem fio, difundida e ubíqua, a partir da popularização dos telefones celulares, das redes de acesso à internet sem fio e das redes caseiras de proximidade com a tecnologia Bluetooth. (FREIRE e BATISTA, 2014, p. 49)

Existem inúmeros debates sobre os malefícios e os benefícios de se viver em uma Era Digital. Há de se falar nas questões de exclusão e analfabetismo digital, bem como nas possíveis consequências para os nativos digitais, a população nascida inteiramente na Era Digital. Ademais, o ambiente virtual é um vasto campo para que criminosos possam cometer atos ilícitos, com brechas de segurança e uma falsa sensação de impunidade por quem está por trás desses atos.

O comportamento virtual tem consequências no mundo real e nesse sentido, não se distingue os dois ambientes, caracterizando uma hiperconectividade. Por isso,

é relevante que o âmbito jurídico se molde constantemente e de forma rápida aos casos concretos que se revelam com a Era Digital.

Os ataques cibernéticos se tornaram uma ameaça frequente, ocorrendo contra empresas, pessoas físicas e países. Uma reportagem da Estadão de 2022 afirmou que tentativas de ataque hacker atingem uma empresa a cada segundo no Brasil (GUIMARÃES e GONSALVES, 2022). A preocupação com cibersegurança é constante diante deste cenário.

Nesse contexto, alguns delitos antes existentes somente no mundo real foram passados também para o meio digital, como o roubo de dados financeiros, clonagem de cartões e jogos de azar. Por outro lado, através desses dispositivos é possível a comunicação com parentes, amigos e ter perfis profissionais, bem como movimentar a economia pelo comércio eletrônico e reduzir custos das empresas.

Para uma melhor contextualização da sociedade da informação é imprescindível mencionar alguns processos pelos quais a humanidade passa: a globalização e a Quarta Revolução Industrial, que contribuíram significativamente para os avanços tecnológicos. Outros aspectos a serem considerados são a origem da internet e a origem do computador.

“A globalização é, de certa forma, o ápice do processo de internacionalização do mundo capitalista”, de acordo com Milton Santos (2006, p. 12). Esse processo não é recente e não existe um consenso entre os pesquisadores sobre quando surgiu a globalização. O que acontece nas esferas econômica, política e social de um país ou região tem efeitos imediatos em outro. Esse fato significa que ocorre interdependência entre essas regiões ou países, mesmo que seus recursos, decisões políticas, desenvolvimento e oportunidades não sejam iguais (UNGERER, 2013).

Conhecida também como Indústria 4.0, a Quarta Revolução Industrial compreende a fusão de várias áreas, envolvendo nanotecnologia, computação quântica, energias renováveis e inteligência artificial. Essa Revolução se torna

diferente das anteriores pela fusão dessas tecnologias e pela interação entre os domínios físicos, biológicos e digitais.

A Internet teve origem através da Agência de Projetos de Pesquisa Avançada (ARPA) do Departamento de Defesa dos Estados Unidos. A primeira rede de computadores se chamava ARPANET e começou a funcionar em 1º de setembro de 1969. Inicialmente, estava aberta para os centros de pesquisa que colaboravam com o Departamento de Defesa dos EUA.

Segundo reportagem da Folha de São Paulo publicada em 2001, “a ARPANET era uma garantia de que a comunicação entre militares e cientistas persistiria, mesmo em caso de bombardeio” (SILVA, 2001). O encerramento das atividades dessa rede de computadores acontece em 28 de fevereiro de 1990.

Em 1983, ocorreu uma divisão e ficou decidido que a ARPANET seria utilizada para fins científicos e que a MILNET teria utilização para aplicações militares. A CSNET e a BITNET foram criadas pela National Science Foundation (NSF) na década de 1980. Nesta mesma década, a ARPA-INTERNET se formou e depois passou a chamar-se INTERNET.

Em 1990, é criada a world wide web (www) pela Centre Europeén poour Recherche Nucleaire (CERN), que possibilita que a internet seja difundida na sociedade em geral. Através da world wide web foi possível que os usuários pudessem ter uma maior facilidade em buscar informações na internet. No Brasil, a internet é iniciada como uma rede acadêmica em 1989.

Por fim, a origem dos computadores tem relação com a necessidade dos seres humanos de desenvolver e aperfeiçoar dispositivos e máquinas para auxiliar em tarefas como contagens e operações aritméticas, bem como na realização de tarefas repetitivas. Era preciso que fossem produzidos dispositivos mais sofisticados para essas funções.

O ábaco foi um dos primeiros dispositivos de computação utilizado para operações aritméticas que surgiu no século XVI a.C, porém necessita de ser

manipulado durante todo o processo de cálculo. A partir de avanços e descobertas ao longo do tempo, foi possível que os computadores ficassem mais parecidos com os dos tempos atuais.

Um dos motivos para a popularização dos computadores foi a criação dos computadores de mesa. A empresa Apple Computer Inc., conhecida atualmente como Apple Inc., foi estabelecida a partir da criação de um computador caseiro comercialmente viável em 1976. Produtos similares foram lançados por empresas como Commodore, Heathkit e Radio Schack. Em 1981, a empresa IBM lançou o seu computador de mesa, que foi nomeado de computador pessoal ou PC.

Diante disso, a sociedade da informação se consolida como um fenômeno global de profunda mudança na organização da sociedade e da economia, de dimensão político-econômica e social, influenciando os indivíduos, as nações e os meios de produção.

3 DIREITOS FUNDAMENTAIS

O artigo 5º da Constituição Federal de 1988 prevê que “todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade”. Os direitos e garantias fundamentais estão divididos no Título II da CF/88 em direitos e deveres individuais e coletivos, direitos sociais, direitos de nacionalidade, direitos políticos e partidos políticos. Segundo Rodrigo Padilha (2020), suas principais características são:

> a)extrapatrimonialidade, uma vez que não são direitos mensuráveis economicamente;
> b)universalidade, pois são aplicados a todos, indistintamente;
> c)inalienabilidade, na medida em que são direitos inegociáveis e intransferíveis, não podendo vender, doar ou ceder os referidos direitos a qualquer título;
> d)imprescritibilidade, posto que não se extinguem pelo desuso, inércia;
> e)irrenunciabilidade: é possível deixar de exercer estes direitos, mas renunciálos, nunca. Um lutador de boxe, por exemplo, abre mão, por tempo determinado, à sua integridade física; porém, a qualquer momento, pode parar de lutar e fazer valer o direito que lhe é inerente;
> f)vinculantes – os poderes públicos devem observar as normas supremas da Constituição, notadamente seus direitos fundamentais;
> g)interdependência – o gozo das liberdades públicas não exclui o exercício de outros direitos, pelo contrário, o usufruto de um direito fundamental pressupõe o gozo simultâneo de outros ou mesmo de todos os direitos fundamentais;
> h)indivisibilidade – todos os direitos fundamentais são merecedores de igual tratamento; não tem como se pensar em igualdade sem falar de liberdade e assim por diante;
> i)historicidade: significa que os direitos fundamentais são históricos, surgiram emblematicamente com a revolução burguesa e evoluíram no correr dos tempos. (PADILHA, 2020, p. 239)

O autor define os direitos fundamentais como “os direitos considerados indispensáveis à manutenção da dignidade da pessoa humana, necessários para assegurar a todos uma existência digna, livre e igual” (PADILHA, 2020, p. 237). Já para Sylvio Motta (2021), a definição é:

> [...] o conjunto de direitos que, em determinado período histórico e em certa sociedade, são reputados essenciais para seus membros, e assim são tratados pela Constituição, com o que se tornam passíveis de serem exigidos e exercitados, singular ou coletivamente. (MOTTA, 2021, p. 211)

Os direitos fundamentais são classificados em direitos fundamentais de primeira geração (ou dimensão), segunda geração (ou dimensão), de terceira

geração (ou dimensão), de quarta geração (ou dimensão) e de quinta geração (ou dimensão). Os de primeira dimensão tiveram origem com a Revolução Francesa em 1789 e Alexandre de Moraes (2022, p.37) os define como “os direitos e garantias individuais e políticos clássicos (liberdades públicas) [...]”. Exemplos: direito à liberdade, à vida, à propriedade, entre outros.

Os de segunda dimensão tiveram origem com a revolução industrial europeia, a partir do século XIX. Nesse momento, as condições de trabalho eram péssimas e movimentos como o cartista na Inglaterra e a comuna na França eclodiram. No início do século XX tem início a Primeira Guerra Mundial e ocorre a busca por direitos sociais. Os direitos de segunda dimensão têm caráter econômico, social e cultural e pode-se citar o direito ao lazer, à saúde, ao trabalho, à assistência social, etc.

Os de terceira dimensão são direitos transindividuais ou metaindividuais, pois vão além do indivíduo e tutelam direitos da sociedade e do gênero humano. Alguns exemplos são o direito à paz, à solidariedade, ao meio ambiente e de comunicação. Os de quarta dimensão são os direitos que englobam a engenharia genética, manipulação genética, biotecnologia e bioengenharia. Pode-se elencar os direitos a democracia, informação e pluralismo.

Para Padilha (2020), os de quinta dimensão são os relativos a questões do ambiente virtual e podem ser a tutela de software, proteção de crimes virtuais e direito autoral na internet. Sobre o ambiente virtual, é significativo mencionar os seguintes direitos constitucionais: proteção de dados pessoais, privacidade, liberdade de expressão e o de sigilo da correspondência, da comunicação e dos dados.

3.1 Proteção dos dados pessoais

Com a promulgação da Emenda Constitucional (EC) 115/2022 em 10 de fevereiro de 2022, houve a alteração da CF/88 para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Segundo reportagem da Câmara dos Deputados, o senador e presidente do Congresso Nacional Rodrigo Pacheco (PSD-MG) afirmou que a medida fortalece o princípio da liberdade e mostra o compromisso da nação com o valor inegociável da liberdade individual (Câmara dos Deputados, 2021). O art. 5º da CF/88 passou a ter incluído o seguinte inciso em sua redação: “LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais” (BRASIL, 1988).

3.2 Privacidade

O direito à privacidade foi incluído com a promulgação da Constituição Federal de 1988 e está previsto no art. 5º, X, da Carta Magna: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988).

Sobre o direito à privacidade, Alexandre de Moraes (2022) afirma que:

> [...] a defesa da privacidade deve proteger o homem contra: (a) a interferência em sua vida privada, familiar e doméstica; (b) a ingerência em sua integridade física ou mental, ou em sua liberdade intelectual e moral; (c) os ataques à sua honra e reputação; (d) sua colocação em perspectiva falsa; (e) a comunicação de fatos relevantes e embaraçosos relativos à sua intimidade; (f) o uso de seu nome, identidade e retrato; (g) a espionagem e a espreita; (h) a intervenção na correspondência; (i) a má utilização de informações escritas e orais; (j) a transmissão de informes dados ou recebidos em razão de segredo profissional.(MORAES, 2022, p. 91).

3.3 Liberdade de expressão

O direito à liberdade de expressão está previsto no art. 5º, inc. IX, o qual afirma que “é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença” (BRASIL, 1988). Além de estar previsto na Constituição, também está previsto em normas supranacionais, como o Pacto de São José de Costa Rica. Tarcisio Teixeira (2022, p.32) afirma que “o exercício da liberdade de expressão pode trazer algum prejuízo para a privacidade. O contrário também é verdadeiro: a preservação da privacidade pode trazer perdas à liberdade de expressão [...].”

3.4 Sigilo da correspondência, da comunicação e dos dados

Para Alexandre de Moraes (2022):

> O preceito que garante o sigilo de dados engloba o uso de informações decorrentes da informática. Essa nova garantia, necessária em virtude da existência de uma nova forma de armazenamento e transmissão de informações, deve coadunar-se com as garantias de intimidade, honra e dignidade humanas, de forma que se impeçam interceptações ou divulgações por meios ilícitos. (MORAES, 2022, p.77)

O art. 5º, inc. XII prevê que “é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal” (BRASIL, 1988).

4 LEGISLAÇÃO BRASILEIRA

É fundamental que o direito acompanhe a nova realidade proporcionada pela Era Digital com o objetivo de garantir a segurança das relações jurídicas, inibir ações delituosas e impedir a prática da “justiça com as próprias mãos”. A transformação digital permitiu benefícios nas relações entre as pessoas, porém também colocou em risco a preservação de uma ordem social justa. Sobre o direito digital, Patricia Peck (2021) afirma que:

> Significam que são os novos profissionais do Direito os responsáveis por garantir o direito à privacidade, a proteção do direito autoral, do direito de imagem, da propriedade intelectual, dos royalties, da segurança da informação, dos acordos e parcerias estratégicas, dos processos contra hackers e muito mais. Para isso, o Direito Digital deve ser entendido e estudado de modo a criar novos instrumentos capazes de atender a esses anseios. (PECK, 2021, p. 26)

Nessa perspectiva, a mesma autora afirma que as relações comerciais migraram para a internet, envolvendo pessoas, empresas, governos e instituições (PECK, 2021, p.26). O relativo anonimato proporcionado pela internet fez com que crescessem os crimes, as reclamações devido a infrações ao Código de Defesa do Consumidor, às infrações à propriedade intelectual, marcas e patentes, entre outros. Também aumentaram os riscos relativos à segurança da informação, concorrência desleal, plágio, sabotagem por hacker, entre outros.

Tarcisio Teixeira (2022, p.234) explica que há enorme expectativa para uma adequada normatização que trate da informática, especialmente no campo criminal. O Código Penal tem sido utilizado para crimes virtuais que têm ausência de legislação específica e os que não estão enquadrados nos tipos penais, são considerados atípicos e portanto, o criminoso fica impune. Existem projetos de Lei no Congresso Nacional que buscam disciplinar as práticas ilícitas que estão surgindo a partir da informática.

Ademais, existem debates sobre as lacunas legislativas a respeito desse assunto, as leis obsoletas e os limites da restrição da liberdade de expressão. Conforme explanado por Auriney Brito (2013, p.17), “no Brasil há apenas uma pequena deficiência que precisa ser sanada pelo Poder Legislativo, que é a proteção jurídica dos bens que compõe a segurança do sistema informático”. Em

contrapartida, é relevante que a legislação referente aos crimes digitais seja elaborada de forma a não acabar punindo inocentes.

Atualmente, as principais leis acerca do ambiente virtual no Brasil são: Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), Lei nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckmann), Lei nº 14.155, de 27 de maio de 2021 e Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), que terá capítulo específico.

4.1 Marco Civil da Internet

Em 2013, o ex-técnico da CIA Edward Snowden fez revelações sobre o programa de espionagem dos Estados Unidos. Este programa incluía monitoramento de conversas da ex-presidente Dilma Rousseff com seus assessores, de milhões de ligações e e-mails de brasileiros e estrangeiros em trânsito no Brasil e espionagem de organizações como a Petrobras e Ministério de Minas e Energia. Esse fato fez com que o Brasil buscasse uma forma de reação aos acontecimentos e uma dessas formas foi a retomada do debate sobre o projeto de lei do Marco Civil da Internet.

O Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014) permitiu que fossem estabelecidos parâmetros para o uso da Internet no Brasil. Foi criado para que não existissem decisões judiciais conflitantes e contraditórias no meio ambiente digital e é conhecida como “Constituição da Internet”. Para Christiany Conte e Celso Fiorillo (2016, p.71), o Marco Civil da Internet é muito mais principiológico do que regulamentador, pois reconhece direitos fundamentais que já estão na Constituição Federal de 1988 ou que já estão em documentos internacionais nos quais o Brasil já é signatário.

É relevante mencionar que sua redação trata dos princípios, garantias, direitos e deveres para o uso da Internet no Brasil, bem como sobre as diretrizes a serem seguidas pelo Poder Público e regras a serem cumpridas por agentes que operam a internet, como aplicações de internet e provedores de conexão. Essa norma surgiu a partir do PL n. 2.126/2011, que foi aprovado em 23 de abril de 2014

e entrou em vigor em 23 de junho de 2014. Sua elaboração teve início em 2009 a partir de colaboração do Ministério da Justiça e do Centro de Tecnologia e Sociedade, da Fundação Getúlio Vargas.

O Marco Civil da Internet também teve a colaboração da sociedade civil através de participação direta e de representantes de diversos setores, 7 (sete) audiências públicas e seu conteúdo foi colocado no portal e-Democracia para que usuários da internet participassem, fazendo sugestões e propostas. Não foram apenas considerados os comentários feitos formalmente, como também os feitos em redes sociais e em posts de blogs.

Desse modo, o processo de elaboração desta Lei teve amplo diálogo entre representantes e representados e é reconhecida por avanços em seu conteúdo. Tarcisio Teixeira (2022, p.41) diz que pode-se extrair do Marco Civil da Internet três grandes pilares: a garantia à liberdade de expressão, a inviolabilidade da privacidade e a neutralidade no uso da internet.

A neutralidade de rede se refere a questão de que quaisquer pacotes de dados devem ser tratados de forma igual pelo responsável pela transmissão do conteúdo, sem distinção por conteúdo, origem e destino. O art. 9º desta Lei discorre sobre isso: “o responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação” (BRASIL, 2014). Nesse caso, a concorrência e a liberdade de circulação de dados e informações na rede são promovidas.

A inviolabilidade da privacidade é garantida, pois a norma trata do sigilo da vida privada do usuário e das suas comunicações feitas pela internet, como demonstrado pelo art. 7º. José Cardozo (2014) diz que o texto é inovador nos aspectos de remoção de conteúdos da internet e responsabilidade de intermediários. O usuário também deve ser informado sobre a coleta e tratamento de seus dados pessoais.

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; (BRASIL, 2014)

Além disso, o art. 8º assegura ao usuário da internet a liberdade de expressão, que também é um direito assegurado pela Constituição Federal de 1988 em seu art. 5º, IX. Dado isso, o usuário pode se manifestar de forma intelectual, artística, científica e na comunicação, não dependendo de licença ou censura. "Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet" (BRASIL, 2014).

4.2 Lei Carolina Dieckmann

A Lei nº 12.737, de 30 de novembro de 2012, também conhecida como Lei Carolina Dieckmann, prevê sobre a tipificação criminal de delitos informáticos. A Lei ficou assim conhecida pois a atriz de mesmo nome teve suas fotos íntimas divulgadas na internet através de uma obtenção ilegítima, após uma manutenção técnica em seu computador. Tendo também recebido ameaças e extorsão para que essa divulgação não fosse feita pelos criminosos. O trâmite do PL. n 35/2012 foi acelerado após esse caso, que teve repercussão na mídia e não teve amparo de uma legislação específica na época. Moisés Cassanti (2014) esclarece que:

> *[...] Lei 12.737/12*, criminaliza as condutas cometidas através da internet, tais como: invasão de computadores, roubo e/ou furto de senhas e de conteúdos de e-mails e a derrubada intencional de sites, inclusive oficiais, o que tem ocorrido em todo o mundo. Esta lei ganhou o apelido de *Lei Carolina Dieckmann* porque o projeto (PL 35/12) foi elaborado na época em que as fotos da atriz foram espalhadas pela internet. (CASSANTI, 2014, p. 131)

Esta norma acrescentou ao Código Penal os artigos 154-A e 154-B e alterou a redação dos artigos 266 e 298. O art.154-A introduziu a tipificação do delito de invasão de dispositivo informático, o art. 154-B previu sobre a sua devida ação penal e os arts. 266 e 298 foram alterados de forma a gerar consequências penais em situações que antes não geravam por não terem uma previsão específica. O cartão de crédito ou débito foi equiparado a documento particular passível de falsificação através do parágrafo único do art. 298.

Em 2022, a Lei completou 10 anos e em reportagem da Defensoria Pública Geral do Estado do Ceará foi dito que a Lei nº 12.737/2012 é considerada a principal ferramenta legal para a segurança virtual dos brasileiros (Defensoria Pública Geral do Estado do Ceará, 2022). Também existem críticas a respeito da norma, porém com o seu advento houve um avanço na criação de dispositivos legais sobre crimes cibernéticos.

Algumas críticas apontadas sobre a Lei Carolina Dieckmann são: pena branda no que tange a pena máxima, a questão do legislativo ainda discutir outros projetos de lei que tratam sobre a divulgação de conteúdo íntimo na internet como a Lei 13.718/18, o PL n. 35/2012 não ter sido debatido suficientemente antes de sua aprovação e falta de capacitação técnica para apurar os crimes.

4.3 Lei nº 14.155/2021

A lei nº 14.155, de 27 de maio de 2021, alterou o Código Penal para tornar mais graves os crimes de violação de dispositivo informático (art. 154-A), furto (art.155) e estelionato (art. 171) cometidos de forma eletrônica ou pela internet. Também alterou o Código de Processo Penal para definir a competência em modalidades de estelionato (art. 70). Anteriormente, o art. 154-A (introduzido pela Lei nº 12.737/2012) tinha a seguinte redação:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> (...)
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (BRASIL, 2012)

Após a Lei nº 14.155/2021, a redação passou a ser:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou

> informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> .....
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
> § 3º .....
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. (BRASIL, 2021)

Com isso, pode-se observar que a redação do caput foi alterada e sua pena prevista foi aumentada, sendo agravada para reclusão. Além disso, as frações da causa de aumento do § 2 e a pena cominada à qualificadora do § 3 também foram aumentadas. Em relação ao furto (art. 155), a Lei incluiu o § 4º-B, que descreve uma nova qualificadora e o §4º-C, que prevê duas causas de aumento ao § 4º-B:

> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
> I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
> II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável. (BRASIL, 2021)

No art. 171 (estelionato), foram incluídos o § 2º-A (uma nova qualificadora) e § 2º-B (causa de aumento ao § 2º-A), como também as frações foram alteradas e a abrangência da causa de aumento foi ampliada no § 4º.

> Art. 171. .....
> .....
> Fraude eletrônica
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.
> .....
> Estelionato contra idoso ou vulnerável
> § 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso. (BRASIL, 2021)

Também houve a inclusão do § 4º no art. 70 do Código de Processo Penal:

> § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção. (BRASIL, 2021)

A partir disso, foram incluídas regras de competência com relação ao delito de estelionato.

5 CONVENÇÃO DE BUDAPESTE

A Convenção de Budapeste ou a Convenção sobre o Crime Cibernético é um tratado internacional de direito penal e processo penal elaborado pelo Comitê Europeu para os Problemas Criminais, com o apoio de uma comissão de especialistas. Foi celebrado em Budapeste, na Hungria, em 23 de novembro de 2001 e também foi o primeiro tratado internacional sobre os crimes cibernéticos, elaborado pelo Conselho da Europa.

O Conselho da Europa teve origem em 1949 e tem a finalidade de fomento da cooperação internacional, a defesa dos princípios de liberdade moral e política, do progresso social econômico e da superioridade do Direito. É a mais antiga organização política europeia em atividade, engloba 46 (quarenta e seis) países e tem 6 (seis) Estados como observadores.

A celebração da Convenção, em novembro de 2001, ocorreu após o atentado terrorista de 11 de setembro de 2001 nos Estados Unidos. A comunicação dos terroristas da *Al-Qaeda* aconteceu através de rascunho de uma caixa de correio eletrônico não enviada. Por esse motivo, não houve interceptação pelo Pentágono, o Departamento de Defesa dos Estados Unidos.

Mais de 60 países já aderiram ao tratado e 158 a utilizam como orientação para as legislações locais. O convite para a adesão ao tratado pelo Brasil foi em dezembro de 2019 e o país aprovou a adesão em dezembro de 2021, através do Decreto Legislativo nº 37. A Convenção é dividida em quatro capítulos, que Marcelo Crespo (2011) sintetiza da seguinte forma:

> a) Capítulo I. Abarca questões relativas a incriminações de certas condutas, definindo nove tipos de infrações, subdivididas em quatro categorias. Há previsão das seguintes infrações: acesso ilícito, interceptação ilícita, interferência nos dados, interferência nos sistemas, utilização indevida de equipamentos, falsificação relacionada com computadores, fraudes relacionadas com computadores, pornografia infantil e infrações a direitos de autor;
> b) Capítulo II. Trata do Direito Processual determinando as condições e salvaguardas gerais relativas às provas, estabelecendo condições de armazenamento de informações, divulgação parcial de dados de tráfego, investigação e apreensão de dados informatizados e, ainda, interceptação de dados;

> c) Capítulo III. Relativo a ações de cooperação internacional, inclusive quanto à extradição. Prevê duas formas de entendimento político-jurídico dos subscritores, conforme haja base jurídica vinculante entre as partes (como um acordo ou tratado) ou não. No primeiro caso, aplica-se o que fora convencionado entre as partes;
> d) Capítulo IV. Contém as cláusulas finais, comuns aos tratados internacionais. (CRESPO, 2011, p. 31)

Assim, pode-se extrair deste tratado internacional questões relativas a criminalização de condutas, normas para investigação, produção de provas eletrônicas e meios de cooperação internacional, como extradição e assistência jurídica mútua. Auriney de Brito (2013) resume que os três objetivos específicos da Convenção de Budapeste são:

> [...] (a) harmonizar a tipicidade penal no ambiente do ciberespaço pelos Estados signatários; (b) definir os elementos do sistema de informática promovendo a unidade na interpretação da legislação penal interna e possibilitar a credibilidade da prova eletrônica no ambiente virtual; (c) implementar um sistema rápido e eficaz de cooperação internacional no combate à criminalidade de informática.(BRITO, 2013, p. 19)

Dado isso, a Convenção sobre o Crime Cibernético representa importante instrumento para viabilizar a cooperação internacional e a investigação no que tange aos crimes praticados por meio da internet e dos computadores. Considerando-se que os crimes virtuais são uma realidade nos países do mundo e que o aumento do uso da internet tem influenciado na cibercriminalidade.

6 CRIMES CIBERNÉTICOS

Em 2021, de acordo com um ranking da consultoria alemã Roland Berger, o Brasil é o 5º maior alvo de crimes cibernéticos, ficando somente atrás dos EUA, Reino Unido, Alemanha e África do Sul (ÉPOCA NEGÓCIOS, 2021). Esse estudo demonstra que os crimes cibernéticos em sido razão de prejuízos econômicos ao redor do mundo, tanto para pessoas físicas como para pessoas jurídicas. Com o dinamismo da atual sociedade, os criminosos tendem a utilizar técnicas cada vez mais sofisticadas e danosas.

O valor correspondente às perdas globais, neste mesmo ano, podem chegar a US$ 6 trilhões, o que corresponde a três vezes o Produto Interno Bruto (PIB) do Brasil. Segundo reportagem da Época Negócios, “o levantamento da Roland Berger aponta que o país já ultrapassou o volume de ataques do ano passado apenas nesse primeiro semestre [...] ”(ÉPOCA NEGÓCIOS, 2021).

Como elucida Spencer Sydow (2015, p.25), os crimes informáticos tem características próprias que os diferencia dos crimes do mundo real. O autor cita que não existe o contato físico entre vítima e ofensor, não exige que o agressor visite previamente o local para cometimento do fato, ocorre em ambiente onde não há governo, povo ou território, não há padrões para seu acontecimento, não implica aparentemente em altos riscos e não gera sensação de violência (SYDOW, 2015).

Esse tipo de crime tem se tornado frequente com a utilização da internet, redes sociais e de dispositivos informáticos. O seu alcance é exponencial, pois o criminoso é capaz de obter informação de vários clientes de uma organização. A doutrina utiliza também outras nomenclaturas como ‘crimes virtuais’, ‘crimes de computador’, ‘crimes eletrônicos’, ‘delitos informáticos’, ‘crimes cibernéticos’, etc.

Esses delitos são explicados por Celso Fiorillo e Christiany Conte (2016, p.61) como “situações nas quais há o uso do computador para a prática do ilícito penal, bem como as práticas criminosas contra o computador ou em relação às informações contidas na máquina”. Essa modalidade de delito não tem somente os

computadores como meio para a sua prática, mas também a telefonia, a nanotecnologia, a robótica, a internet e outras ferramentas tecnológicas.

Grande parte dos crimes cibernéticos se propagaram nas décadas de 1980 e 1990 e era mais comum a disseminação de vírus, pornografia infantil, invasão de sistemas e a pirataria. Atualmente, os crimes virtuais mais comuns são: apologia ao crime, malware, ato obsceno, calúnia, difamação, divulgação de material confidencial, estupro virtual, perfil falso, injúria, phishing, spam, etc.

Em janeiro de 2022, o número de usuários ativos na internet no mundo se aproximou de 5 bilhões de pessoas, ou seja, quase 63% da população do mundo (INSPER, 2022). A internet traz uma falsa sensação de impunidade para os autores dos crimes em razão do anonimato, o que não corresponde a realidade.

Em reportagem do Jornal da USP, o professor Daniel Pacheco Pontes afirma que a legislação atual, se aplicada corretamente, possui os mecanismos necessários para garantir a investigação e punição dos crimes cometidos pela internet (JORNAL DA USP, 2022). No atual contexto mundial, nossas atividades são rastreadas fora e dentro da vida online. Para Marcelo Crespo (2019):

> Sobre isso, todas as vezes que fazemos compras online utilizando nossos cartões de crédito, que nos inscrevemos em uma newsletter ou nos registramos em um site, buscamos por um apartamento ou carro, ou até mesmo falamos em voz alta sobre um novo curso que gostaríamos de fazer, estamos inadvertidamente deixando uma pista sobre quem somos e sobre o que fizemos.(CRESPO, 2019, p.1)

Por outro lado, a internet pode ser segmentada em surface web, deep web e dark web. Esse fato amplia a discussão sobre a investigação da autoria dos crimes cibernéticos. A surface web é a parte da internet na qual se utiliza canais de busca como o Google e o Bing e também pode-se utilizar navegadores como o Google Chrome. Representa cerca de 4% de toda a internet e é por onde a maior parte das pessoas acessa a internet.

A deep web representa mais de dois terços da internet e é utilizada para a divulgação de conteúdos de forma anônima. Os sites são não indexados e não é possível localizá-los por canais de busca, como o Bing e o Google. Nem sempre

essa parte da web é utilizada para o cometimento de atos ilícitos, porém muitos crimes cibernéticos são praticados nesse ambiente.

A dark web é uma pequena parte da deep web, onde atividades ilegais, como tráfico de drogas e pedofilia, são muito comuns. Ocorre também maior dificuldade para que a polícia encontre os responsáveis por esses atos em razão da criptografia bastante complexa e do anonimato (KOZCIAK, 2021).

Também é pertinente mencionar que existem algumas características presentes no ciberespaço que permitem a vulnerabilidade para o cometimento de delitos, citadas por Marcelo Crespo (2011) que, de forma sucinta, consistem na:

> Capacidade de processar, guardar e circular, de forma automatizada e em tempo real, grandes quantidades de informações em formato digital dos mais variados (fotos, filmes, sons)[...];
> O número enorme de usuários, a frequência com que acessam, a liberdade que têm para enviar, transferir, difundir e acessar informações[...];
> As próprias características físicas, técnicas e lógicas das TIC, que podem ser acessadas de forma ilegítima, tendo seu conteúdo alterado[...];
> A enorme potencialidade de multiplicação das ações ilícitas.(CRESPO, 2011, p. 20)

6.1 Principais crimes cibernéticos

Patrícia Carolina Kozciak (2021) elenca e explica os tipos mais comuns de crimes digitais que são praticados através da internet:

> Apologia ao crime — incitar publicamente a prática de crime, fazer, publicamente (art. 287 “Apologia de fato criminoso ou de autor de crime” — Código Penal — Decreto-Lei no 2.848, de 7 de dezembro de 1940).
> Aplicativos maliciosos (malware) — são programas maliciosos instalados sem permissão do usuário, como vírus, para realização de furtos de dados pessoais, para fins fraudulentos.
> Ato obsceno — praticar ações de natureza sexual com ofensa ao pudor.
> Calúnia — atribuir sem provas a alguém uma ofensa que afete a sua dignidade ou acusar alguém de um crime.
> Crimes virtuais contra mulheres — envolvem casos de perseguições, ofensas, difamação, assédio e também a distribuição de fotos e vídeos pessoais.
> Crimes de ódio — são ataques racistas, de gênero, misóginos e até terroristas.
> Difamação — atribuir a alguém uma acusação pública que afete a sua reputação.
> Divulgação de material confidencial — expor publicamente dados de terceiros sem autorização (art. 153 “Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de

> que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem" — Código Penal — Decreto-Lei no 2.848/1940).
> Estupro virtual — envolve coação para produção de conteúdo sexual sob ameaça de divulgação de fotos e vídeos.
> Formulários falsos — envio de mensagens de e-mail falsas para os usuários solicitando que seja preenchido um formulário, assim, os criminosos conseguem várias informações sobre os usuários, incluindo dados bancários.
> Injúria — atribuir a alguém uma ofensa desonrosa que afete a sua dignidade.
> Lojas virtuais falsas — é um golpe com a divulgação de ofertas falsas, com preços muito abaixo do preço real de produtos, no qual os usuários adquirem os produtos, realizam o pagamento, mas não recebem as mercadorias.
> Pedofilia — envolve armazenamento, produção, troca, publicação de vídeos e imagens contendo pornografia infantil ou do adolescente, cometido pela Internet.
> Perfil falso — refere-se usuários que criam identidade falsa na Internet para usar redes sociais, aplicar golpes ou realizar fraudes.
> Phishing — refere-se a conversas ou mensagens falsas com links fraudulentos.
> Plágio — é a cópia de informações veiculadas por terceiros sem a indicação da fonte.
> Preconceito ou discriminação — envolve utilizar sites da Internet ou redes sociais para opinar, de forma pejorativa e negativa, envolvendo assuntos como etnia, religião, opção sexual, raças, entre outros.
> Spam — são mensagens enviadas sem o consentimento do usuário. (KOZCIAC, 2021, p. 184 e 185)

6.2 Classificação

Damásio de Jesus e José Milagre (2016, p.22) classificam os crimes informáticos como crimes informáticos próprios, crimes informáticos impróprios, crimes informáticos mistos e crime informático mediato ou indireto.

Os crimes informáticos próprios são aqueles em que o bem jurídico ofendido é a tecnologia da informação em si. Ao passo que, nos crimes informáticos impróprios a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal Brasileiro.

Existe a proteção do bem jurídico informático e a proteção de outro bem jurídico nos crimes informáticos mistos. Por fim, o crime informático mediato ou indireto é aquele em que o delito informático é praticado para a ocorrência de um delito não informático consumado ao final.

De forma diferente, Marcelo Crespo (2011, p.24) classifica os crimes digitais somente como próprios e impróprios. O autor define que nos crimes digitais próprios,

os bens jurídicos atingidos são os sistemas informatizados ou de telecomunicações ou dados. Os crimes digitais impróprios são os que já estão tipificados no ordenamento, mas que agora são praticados com auxílio de modernas tecnologias.

Crespo (2011) traz exemplos e afirma que os crimes digitais próprios são os de acesso não autorizado, obtenção e transferência ilegal de dados, dano informático, de vírus e sua disseminação, divulgação ou utilização indevida de informações, embaraçamento ao funcionamento de sistemas, engenharia social, phishing e interceptação ilegal de dados.

Os crimes digitais impróprios têm como modalidades mais comuns a ameaça, a participação em suicídio, incitação e apologia ao crime, falsa identidade e falsidade ideológica, violação de direitos autorais, pornografia infantil e crimes contra a honra.

6.3 Sujeito ativo e sujeito passivo

De acordo com o Decreto-Lei nº 3.914, de 9 de dezembro de 1941, crime pode ser considerado como “a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa” (BRASIL, 1941). Rogério Greco (2022, p.199) traz o conceito material de crime como “toda conduta que viole (ou ameace) os bens jurídicos mais importantes e necessários ao convívio em sociedade”.

O sujeito ativo é a pessoa que pratica a conduta descrita pelo tipo penal, segundo Guilherme Nucci (2022, p.312). Por faltar o elemento vontade, animais e coisas não podem ser sujeitos ativos de crimes. Em relação aos crimes cibernéticos, os sujeitos ativos podem ser os hackers, os crackers, os carders, os lammers, os wannabes, os phreakers e os white e black hats.

Os hackers são programadores que não tem intenções ilegítimas, ou seja, pode ser um profissional de segurança ou um pesquisador. Invadem sistemas, porém não com intenção de danificá-lo. Essa nomenclatura surgiu no MIT (Massachusetts Institute of Technology), quando estudantes realizavam testes sobre o que podia ser feito com o computador.

Crackers deriva do inglês ‘to crack’ que significa quebrar. Esse tipo de sujeito ativo quebra um sistema de segurança para que possa invadi-lo. Utilizam seus conhecimentos de informática para finalidades ilícitas, como roubo de dinheiro, informações e quebra de códigos de criptografia. São considerados criminosos.

Os carders roubam informações de cartões de crédito, contas bancárias, cartões de conta poupança ou corrente para que possam fazer compras pela internet. Praticam o crime de estelionato. Os lammers se autodenominam hackers, porém possuem pouco conhecimento sobre as práticas dos hackers. Os wannabes possuem mais conhecimento que os lammers.

Os phreakers atuam na telefonia. Podem fazer escuta telefônica, utilizar telefonia em nome de terceiros, realizar interceptações, etc. Os black hats são crackers e utilizam seus conhecimentos de informática para atos ilícitos. Os white hats são conhecidos como hackers éticos e usam esses conhecimentos para melhorar a segurança dos sistemas.

Nucci (2022, p.317) explica que “sujeito passivo é o titular do bem jurídico protegido pelo tipo penal incriminador, que foi violado”. Nos crimes cibernéticos, o sujeito passivo pode ser qualquer pessoa física ou jurídica que acessa um computador, com ou sem internet. Dado isso, as possíveis vítimas dessa modalidade de delito são aquelas que estão conectadas a um computador.

6.4 Métodos

Os sujeitos ativos dos crimes virtuais tendem a desenvolver diversas formas para atingir as possíveis vítimas. Alguns meios utilizados são conteúdos enviados através de e-mail, aplicativos de mensagens, páginas falsas da internet, sistemas de compartilhamento de arquivos (P2P) e arquivos PDF. São exemplos de técnicas utilizadas pelos criminosos: vírus, worms, trojan, spyware, ransomware, phishing e engenharia social.

Felipe Machado (2014) define vírus como um pequeno programa escrito que tem como objetivo, sem a permissão ou conhecimento do usuário, alterar a forma

como um computador opera. Os vírus podem danificar o computador, apagar arquivos, formatar o disco rígido, interferir na memória do computador, fazer com o equipamento fique mais lento, etc.

Da mesma forma que os vírus, os worms “infectam” computadores. Porém, diferentemente dos vírus, podem se autopropagar através da rede de computadores e não necessitam de interação humana. O spyware é um programa que monitora as atividades de um usuário e envia a terceiros. Esse malware pode salvar senhas e informações pessoais.

O trojan ou cavalo de troia é, segundo Damásio de Jesus e José Milagre (2016, p.15), “uma instrução ou código malicioso comumente ocultado em outro software, que, instalado, torna um computador ou sistema vulnerável ou mesmo explora vulnerabilidades já existentes”. O cavalo de troia precisa ser instalado pelo usuário do computador e quando seus códigos maliciosos são ativados, pode roubar dados, senhas de acesso, etc.

O ransomware é um malware que bloqueia o computador e pede uma taxa para o resgate. Podem se infiltrar através de links enviados por e-mail, redes sociais e sites. A técnica de phishing necessita que a vítima tenha acesso a sites fraudulentos, preencha formulários ou faça download de um malware para que os criminosos tenham acesso a informações da vítima.

Os sujeitos ativos dos delitos também recorrem a engenharia social para enganar e persuadir as vítimas. O golpista pode simular ser uma instituição, outra pessoa ou um profissional para induzir a vítima a fornecer informações sigilosas ou a realizar determinada ação. Dessa forma, consegue infectar computadores e obter dados.

7 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A Lei nº 13.709, de 14 de agosto de 2018, ou Lei Geral de Proteção de Dados Pessoais (LGPD) foi inspirada na General Data Protection Regulation (GDPR). A GDPR é o Regulamento Geral de Proteção de Dados Pessoais Europeu n. 679, que foi aprovado em 27 de abril de 2016 e aborda a proteção das pessoas físicas no tratamento dos dados pessoais e na livre circulação desses dados. Por esse motivo, países e empresas que tenham relações comerciais com a União Europeia precisam se adequar a GDPR e ter uma Legislação no mesmo nível.

Patricia Peck (2021, p.10) esclarece que “o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da UE”. A LGPD é a Lei que dispõe sobre o tratamento de dados pessoais no Brasil e que foi promulgada em 2018, porém já estava sendo discutida há oito anos no Congresso Nacional. Anteriormente, já era possível encontrar legislações que tratavam sobre esse tema, como a Constituição Federal de 1988 e o Código de Defesa do Consumidor, porém a LGPD se revela específica e exclusiva.

A Lei Geral de Proteção de Dados Pessoais possui 65 artigos, 10 capítulos e tem o objetivo de proteger “os direitos fundamentais de liberdade e de privacidade e o de livre desenvolvimento da personalidade da pessoa natural”. Em publicação, o Conselho de Justiça Federal (CJF) afirmou que “representa importante avanço na consolidação dos direitos do cidadão e grande desafio para as instituições se adequarem aos dispositivos estabelecidos por este normativo”. Em seu art. 2º estão previstos os fundamentos da disciplina da proteção de dados pessoais:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018)

Outro fator fundamental para a compreensão desta Lei são as seguintes terminologias:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> [...]
> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
> [...]
> XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (BRASIL, 2018)

7.1 As empresas e a LGPD

A temática de proteção de dados se revela atual e um dos exemplos é o vazamento de dados referentes a informações de mais de 87 milhões de pessoas de todo o mundo em 2018, quando a empresa Cambridge Analytica teve acesso a esses dados através de um aplicativo de teste psicológico no Facebook chamado “This is Your Digital Life” .

A finalidade foi fazer propaganda política e não teve consentimento dos usuários. Essa questão colocou em evidência o compromisso do Facebook com a proteção de dados dos usuários e o valor da empresa diminuiu US$ 35 bilhões. Isso demonstra como o vazamento de dados pode impactar uma empresa.

Referente a esse caso, no Brasil, em decisão da Secretaria Nacional do Consumidor (Senacon), órgão vinculado ao Ministério da Justiça e Segurança Pública, a empresa foi condenada ao pagamento de uma multa de R$ 6,6 milhões pelo vazamento de dados de usuários brasileiros (GOV, 2022).

Em 2022, segundo relatório da IBM Security (X-Force Threat Intelligence Index 2023), o Brasil representou 67% dos casos atendidos pela X-Force na

América Latina e foram mais comuns o roubo de dados (32%), vazamento de dados (22%) e a destruição de dados (22%) (JORNAL DIA DIA, 2023).

A ocorrência de um vazamento de dados pode produzir desgaste a imagem e a reputação da empresa, além de consequências como multas e problemas judiciais para a organização. Nesse contexto, o processo de adequação a Lei Geral de Proteção de Dados também pode apresentar desafios.

Nesse sentido, Patricia Peck Pinheiro e Larissa Lotufo (2021, p.33 a 40) pontuam sobre as melhores práticas em proteção de dados. As autoras citam a adoção de uma política de segurança de informação sólida, ou seja, implementar um Sistema de Gestão de Segurança da Informação (SGSI) e definir bem os atores responsáveis pela proteção de dados na organização (controlador, operador e encarregado).

Também assegurar a execução dos direitos dos titulares de dados (acesso, alteração, eliminação, revogação de consentimento, não discriminação no uso de dados, revisão de decisões automatizadas), adotar a anonimização ou pseudoanonimização dos dados se possível, emitir o Relatório de Impacto de Proteção de Dados (RIPD) como uma prática (obrigação imposta pela LGPD), construir um Comitê de Proteção de Dados e enfocar a figura do DPO (*Data Protection Officer*), como também se atentar às particularidades da transferência internacional de dados (arts. 33, 34, 35 e 36 da LGPD).

7.2 Consequências

Em 27 de fevereiro de 2023, foi publicada a Resolução CD/ANPD Nº 4, de 24 de fevereiro de 2023. Essa Resolução aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas e permite que a Autoridade aplique punições pelo não cumprimento da Lei Geral de Proteção de Dados Pessoais. O art. 53 da LGPD prevê sobre a criação deste Regulamento:

> Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. (BRASIL, 2018)

Por isso, trata da atuação sancionatória da Autoridade Nacional de Proteção de Dados (ANPD). A dosimetria é “o método que orienta a escolha da sanção mais apropriada para cada caso concreto em que houver violação à LGPD e permite calcular, quando cabível, o valor da multa aplicável ao infrator”.

Danilo Doneda (2021, p.467) afirma que “a existência de uma autoridade administrativa que supervisione a aplicação de marcos regulatórios de proteção de dados pessoais é uma tendência fortemente enraizada nessa disciplina”. A Autoridade Nacional de Proteção de Dados (ANPD) é substancial para garantir a eficácia da LGPD, sendo responsável por zelar, implementar e fiscalizar o seu cumprimento em território nacional.

O Regulamento de Dosimetria e Aplicação de Sanções Administrativas é dividido em 3 (três) capítulos e prevê sobre a aplicação das sanções (sanções administrativas, classificação das sanções, aplicação de advertência, aplicação de multa simples), a definição do valor-base, as circunstâncias e a incidência de agravantes e atenuantes, a aplicação da multa diária e o pagamento da sanção de multa.

Também prevê sobre a publicização da infração, bloqueio de dados pessoais, eliminação dos dados pessoais, suspensão parcial do funcionamento de banco de dados, suspensão do exercício de atividade de tratamento dos dados pessoais, proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados e o atendimento ao princípio da proporcionalidade.

As sanções previstas na LGPD são:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;

> [...]
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (BRASIL, 2018)

A aplicação das sanções ocorrerá depois de análise caso a caso através de procedimento administrativo, assegurado o direito à ampla defesa, ao contraditório e ao devido processo legal. Os critérios e parâmetros que devem ser considerados na definição da sanção são: a gravidade e a natureza das infrações e dos direitos pessoais afetados e a boa-fé do infrator.

Também a vantagem auferida ou pretendida pelo infrator, a condição econômica do infrator, a reincidência específica, a reincidência genérica, o grau de dano, a cooperação do infrator, adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, a adoção de política de boas práticas e governança, a pronta adoção de medidas corretivas e a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

O destino da arrecadação das multas será o Fundo de Defesa de Direitos Difusos (FDD), que foi criado a partir da Lei nº 7.347/1985 e tem por finalidade “a reparação dos danos causados ao meio ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico, paisagístico, por infração à ordem econômica e a outros interesses difusos e coletivos”.

7.3 Jurisprudência

O projeto Painel LGPD nos tribunais oferece estudos avançados sobre proteção de dados e direitos fundamentais no Brasil. No estudo sobre o panorama de uso da LGPD foram considerados 5 (cinco) critérios objetivos de relevância: (0) não é decisão judicial; (1) não possui relação com a LGPD; (2) apenas menciona a LGPD; (3) a LGPD é debatida de forma importante, mas não é o ponto central do caso; (4) a LGPD é a questão central do caso. Na jurisprudência do 2º ano (2022) de vigência da Lei, foram analisados mais de 1700 documentos.

Os temas mais recorrentes nos casos analisados foram: pedidos de provas digitais de geolocalização em ações trabalhistas, responsabilidade civil por incidentes de segurança e vazamento de dados, inscrição indevida em cadastro de inadimplentes do Serasa Limpa Nome e direito de revisão no tratamento automatizado de dados pessoais. O gráfico a seguir mostra o quantitativo de capítulos tratados nas decisões relevantes sobre a LGPD:

Quantitativo de capítulos tratados nas decisões relevantes sobre LGPD

	Capítulo prioritário	Decisões
1.	CAP. VI - DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS (III - Da Responsabilidade e do Ressarcimento de Danos)	18
2.	CAP. II - DO TRATAMENTO DE DADOS PESSOAIS (I - Dos Requisitos para o Tratamento de Dados Pessoais)	17
3.	CAP. I - DISPOSIÇÕES PRELIMINARES	17
4.	CAP. I - DISPOSIÇÕES PRELIMINARES, CAP. II - DO TRATAMENTO DE DADOS PESSOAIS (I - Dos Requisitos para o Tratam...	13
5.	CAP. VII - DA SEGURANÇA E DAS BOAS PRÁTICAS (I - Da Segurança e do Sigilo de Dados)	6
6.	CAP. VI - DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS (III - Da Responsabilidade e do Ressarcimento de Danos...	6
7.	CAP. II - DO TRATAMENTO DE DADOS PESSOAIS (I - Dos Requisitos para o Tratamento de Dados Pessoais), CAP. III - DOS...	4
8.	CAP. II - DO TRATAMENTO DE DADOS PESSOAIS (I - Dos Requisitos para o Tratamento de Dados Pessoais), CAP. II - DO T...	4
9.	CAP. I - DISPOSIÇÕES PRELIMINARES, CAP. VI - DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS (III - Da Responsa...	4
10.	CAP. III - DOS DIREITOS DO TITULAR	3
11.	CAP. I - DISPOSIÇÕES PRELIMINARES, CAP. III - DOS DIREITOS DO TITULAR	3
12.	CAP. I - DISPOSIÇÕES PRELIMINARES, CAP. VI - DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS (III - Da Responsa...	3
13.	CAP. I - DISPOSIÇÕES PRELIMINARES, CAP. II - DO TRATAMENTO DE DADOS PESSOAIS (I - Dos Requisitos para o Tratam...	2
14.	CAP. II - DO TRATAMENTO DE DADOS PESSOAIS (I - Dos Requisitos para o Tratamento de Dados Pessoais), CAP. VI - DOS...	2
15.	CAP. II - DO TRATAMENTO DE DADOS PESSOAIS (II - Do Tratamento de Dados Pessoais Sensíveis)	2
16.	CAP. II - DO TRATAMENTO DE DADOS PESSOAIS (II - Do Tratamento de Dados Pessoais Sensíveis), CAP. III - DOS DIREITO...	2
17.	CAP. I - DISPOSIÇÕES PRELIMINARES, CAP. II - DO TRATAMENTO DE DADOS PESSOAIS (I - Dos Requisitos para o Tratam...	2
18.	CAP. IV - DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO (II - Da Responsabilidade)	2
19.	CAP. II - DO TRATAMENTO DE DADOS PESSOAIS (I - Dos Requisitos para o Tratamento de Dados Pessoais), CAP. III - DOS...	2
20.	CAP. III - DOS DIREITOS DO TITULAR, CAP. VII - DA SEGURANÇA E DAS BOAS PRÁTICAS (I - Da Segurança e do Sigilo de D...	2

1 - 20 / 60 < >

Fonte: https://painel.jusbrasil.com.br/#Conclusoes

Nas principais conclusões do estudo, Laura Schertel Mendes afirmou que “A proteção de dados no Brasil tem ganhado maior robustez por parte dos tribunais brasileiros [...]”. O Tribunal de Justiça de São Paulo (TJSP) foi o tribunal com mais decisões relevantes sobre o quantitativo por tribunal onde a LGPD é tema central, isto é, é o tribunal com maior número de decisões sobre proteção de dados em comparação aos demais.

Pode-se observar a seguir 2 (dois) exemplos de jurisprudência com a utilização da Lei nº 13.709/2018 como fundamento:

> LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E DIREITO DO CONSUMIDOR. AÇÃO COM PRECEITOS CONDENATÓRIOS. Sentença de improcedência dos pedidos. Recurso de apelação do autor. Vazamento de pessoais não sensíveis do autor (nome completo, números de RG e CPF, endereço, endereço de e-mail e telefone), sob responsabilidade da ré. LGPD. Responsabilidade civil ativa ou proativa. Doutrina. Código de Defesa do Consumidor. Responsabilidade civil objetiva. Ausência de provas, todavia, de violação à dignidade humana do autor e seus substratos, isto é, liberdade, igualdade, solidariedade e integridade psicofísica. Autor que não demonstrou, a partir do exame do caso concreto, que, da violação a seus dados pessoais, houve a ocorrência de danos morais. Dados que não são sensíveis e são de fácil acesso a qualquer pessoa. Precedentes. Ampla divulgação da violação já realizada. Recolhimento dos dados. Inviabilidade, considerando-se a ausência de finalização das investigações. Pedidos julgados parcialmente procedentes, todavia, com o reconhecimento da ocorrência de vazamento dos dados pessoais não sensíveis do autor e condenando-se a ré na apresentação de informação das entidades públicas e privadas com as quais realizou o uso compartilhado dos dados, fornecendo declaração completa que indique sua origem, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, assim como a cópia exata de todos os dados referentes ao titular constantes em seus bancos de dados, conforme o art. 19, II, da LGPD. Determinação para envio de cópia dos autos à Autoridade Nacional de Proteção de Danos (art. 55-A da LGPD). RECURSO PARCIALMENTE PROVIDO.
>
> (TJSP; Apelação Cível 1000331-24.2021.8.26.0003; Relator (a): Alfredo Attié; Órgão Julgador: 27ª Câmara de Direito Privado; Foro Regional III - Jabaquara - 5ª Vara Cível; Data do Julgamento: 16/11/2021; Data de Registro: 16/11/2021)

> AGRAVO DE INSTRUMENTO. ANTECIPAÇÃO DA TUTELA RECURSAL. AÇÃO CIVIL PÚBLICA. COMERCIALIZAÇÃO DE CADASTRO DE DADOS PESSOAIS. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. CONSENTIMENTO DO TITULAR. DADOS TORNADOS MANIFESTAMENTE PÚBLICOS PELO TITULAR. NÃO OCORRÊNCIA. COMPARTILHAMENTO REMUNERADO. NECESSIDADE DE CONSENTIMENTO ESPECÍFICO. 1. Agravo de instrumento interposto contra decisão proferida em sede de ação civil pública, que indeferiu pedido liminar voltado à suspensão da comercialização de dados pessoais dos titulares por parte do controlador. 2. A Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018 - autoriza o tratamento dos dados pessoais obtidos mediante obtenção do consentimento do titular, dispensando a exigência de consentimento em relação aos dados tornados manifestamente públicos pelo titular, resguardados os direitos deste (art. 7º, inciso I e § 4º). 3. Não evidenciado que o compartilhamento dos dados, na forma como vem sendo feita pelo controlador, se enquadre na hipótese em que a lei prevê a dispensa do consentimento, concede-se a tutela de urgência, nos termos do artigo 300 do CPC, para determinar a suspensão da comercialização de dados pessoais dos titulares, sob pena de multa. 4. Agravo de Instrumento conhecido e provido. Agravo interno prejudicado.
>
> (Acórdão 1341840, 07497652920208070000, Relator: CESAR LOYOLA, 2ª Turma Cível, data de julgamento: 26/5/2021, publicado no DJE: 1/6/2021. Pág.: Sem Página Cadastrada.)

No primeiro caso, o autor alegou que a ré é responsável pela violação de seus dados pessoais e informou ter sofrido constrangimentos, como recebimento de

mensagens, ligações indesejadas em seu celular e diversos e-mails. A fundamentação foi na Constituição Federal, na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), no Código de Defesa do Consumidor e no Código Civil. Por falha de segurança ou falta de modernização de seu sistema, terceiros tiveram acesso a esses dados e os vazaram.

Em síntese, os pedidos foram: a condenação da ré na obrigação de fazer, apresentando a informação das entidades públicas e privadas com as quais realizou o uso compartilhado de seus dados (art. 18, VII, da LGPD) e fornecimento de declaração conforme art. 19, II da LGPD. Também recolher os dados de todos os locais onde foram compartilhados sem autorização (art. 18, parágrafo 6º), ampla divulgação conforme art. 48, parágrafo 2º, I, e art. 52, IV, da LGPD e indenização por danos morais. Em sentença, os pedidos foram julgados improcedentes. Em recurso, os pedidos foram julgados parcialmente procedentes.

No segundo caso, trata-se de um agravo de instrumento interposto pelo MPDFT contra decisão de ação civil pública que indeferiu o pleito liminar voltado à suspensão da comercialização de dados pessoais dos titulares por meio dos produtos “Lista Online” e “Prospecção de Clientes”. O agravante alegou que a comercialização dos dados fere a LGPD, pois existe a necessidade de manifestação específica para cada uma das finalidades para as quais o dado está sendo tratado.

A agravada alegou que os produtos impugnados existem há anos e que não há questionamentos e reclamações dos consumidores. Em decisão foi determinada a suspensão da comercialização dos dados pessoais dos titulares por meio dos produtos “lista online” e “prospecção de clientes”, sob pena de multa de R$ 5.000,00 por venda efetuada, tendo provimento o agravo de instrumento.

8 ATAQUES CIBERNÉTICOS A EMPRESAS

De acordo com reportagem da Valor Econômico, o vazamento de dados provocados por ataques cibernéticos coloca a reputação de empresas em risco, além de provocar perdas financeiras e prejuízo aos consumidores (VALOR ECONÔMICO, 2022). Em alguns países, ataques de ransomware podem provocar o fechamento de mais de 30% dos negócios (FORBES, 2021). Marcos Sêmola (2021) elucida que:

> Baseado em um tipo de software malicioso que adota criptografia e explora ao menos uma das vulnerabilidades encontradas nos perímetros de segurança para ter acesso indevido a dados sensíveis, o ransomware desenha uma cadeia de ataques que explora o vazamento, ameaçando a vítima de publicar suas informações caso o resgate não seja pago, ou de bloquear perpetuamente o acesso a elas, a menos que haja o pagamento de um resgate em ativo financeiro, mais comumente em criptomoeda, para reduzir as chances de rastreamento do criminoso. (SÊMOLA, 2021, pag. 81)

Nos últimos anos, dados de clientes foram alvo de ataques cibernéticos em empresas como Uber (2016), Netshoes (2018), Facebook (2021) e Amazon (2021). Esses dados são obtidos pelas empresas através de operações de transação comercial ou de utilização de serviços. Com o vazamento de dados desses clientes, a empresa pode vir a sofrer multas, advertências, sanções administrativas ou suspensões operacionais (SÊMOLA, 2021).

Além disso, a Lei Geral de Proteção de Dados (LGPD) também pode fazer com que as empresas que tenham os dados vazados e que não consigam provar que não houve a imprudência, imperícia ou negligência no tratamento dos dados pessoais, possam vir a receber advertência, suspensão, multa e exposição pública (SÊMOLA, 2021).

Marcos Tupinambá (2021, p.16 a 26) enumera como formas de ataques a empresas, as técnicas de phishing, malware, ataques em comunicadores instantâneos, golpe do falso boleto, furto de dados por funcionários e terceirizados, botnets, DDoS, armazenamento indevido de dados ilícitos, fraudes em meios de pagamento e formulários web, acessos diretos e indevidos a base de dados e a espionagem industrial e comercial.

Nos ataques em comunicadores instantâneos, o atacante consegue acesso a conta de WhatsApp de um funcionário, por exemplo, com o intuito de aplicar golpes a partir das informações obtidas. Para Tupinambá (2021, p.19), “com a ascensão da comunicação em meio móvel as empresas aderiram pesadamente a essa forma de manter suas equipes em contato, além de atender consumidores e fornecedores”.

No golpe do falso boleto, o criminoso envia um boleto falso para a vítima que é aparentemente legítimo, a vítima paga e descobre depois que é uma fraude. Os golpistas podem infectar um computador com malware para que altere a linha digitável e os código de barras dos boletos e dessa forma, o valor do pagamento é direcionado para a conta desses criminosos.

O furto de dados por funcionários e terceirizados acontece quando funcionários ou terceirizados tem a posse de dados sigilosos ou sensíveis da empresa ou dados de valor econômico e exigem um valor para que não os divulguem. A finalidade é a extorsão de dinheiro da empresa ou passar informações confidenciais para a concorrência.

Os botnets são redes de computadores que estão infectadas por um bot, um vírus mal-intencionado, e que podem ser controlados remotamente por seu criador. Esses computadores são conhecidos como “zumbis”, podendo ser centenas ou milhares de computadores, e o atacante os utiliza para crimes virtuais em larga escala.

Nos ataques DDoS (ataque de negação de serviço), os servidores, banco de dados ou roteador ficam indisponíveis em razão de sobrecarga no serviço informático. O atacante faz com que vários dispositivos, através da botnet, acessem os recursos de um servidor e os usuários legítimos não conseguem acessar esses recursos. No âmbito das empresas, esses ataques têm o objetivo de vantagem competitiva.

No armazenamento indevido de dados ilícitos ocorre armazenamento de conteúdos ilícitos por funcionários da empresa para que sejam distribuídos a outros criminosos, como pornografia infantil e filmes com violação de direitos autorais. Na

espionagem industrial e comercial, as informações de clientes, estratégias de negócios ou produtos e base de dados de uma empresa são buscadas por concorrentes de forma ilícita.

As fraudes em meios de pagamento podem acontecer nas compras de e-commerce da empresa na modalidade cartão não presente. O usuário do cartão o utiliza de forma não presencial e o titular desse cartão só descobre a fraude após receber a fatura ou o aviso de comprar no celular. Com o cartão não presente não é necessário o cartão de crédito físico, apenas os seus dados para a realização do pagamento.

9 CONSIDERAÇÕES FINAIS

Essa pesquisa teve o intuito de analisar como a legislação brasileira pode auxiliar a prevenir ataques cibernéticos a empresas e a pessoas físicas sob o panorama do aumento de casos de crimes cibernéticos e vazamento de dados. Diante disso, foram apontadas as sanções administrativas para as empresas em caso de descumprimento da Lei Geral de Proteção de Dados Pessoais, jurisprudências que utilizaram a LGPD como fundamento e alguns dispositivos para melhores práticas de proteção de dados.

Também fizeram parte da pesquisa: as principais leis sobre o ambiente virtual no Brasil (Marco Civil da Internet, Lei Carolina Dieckmann e Lei nº 14.155/2021), com a explicação geral de seus conteúdos; A mudança trazida com a adesão do Brasil a Convenção de Budapeste ou Convenção sobre o Crime Cibernético; Abordagem sobre os crimes cibernéticos e seus impactos na sociedade, classificação, métodos e sujeito ativo e passivo; Ataques cibernéticos a empresas.

Com isso, nota-se que as empresas devem se adequar a LGPD para minimizar os impactos que um vazamento de dados pode causar, tanto para a organização quanto para pessoas físicas. Observa-se também a partir da pesquisa alguns dispositivos normativos que tratam sobre a punição dos autores de crimes cibernéticos (Código Penal, Lei Carolina Dieckmann, Lei nº 14.155/2021) e o Marco Civil da Internet, que permitiu que fossem estabelecidos parâmetros para o uso da Internet no Brasil.

A partir do presente trabalho foi possível analisar como o Brasil tem avançado em sua legislação para combater uma modalidade de crime cada vez mais frequente na era da informação. Além disso, foi evidenciada como a Lei Geral de Proteção de Dados Pessoais pode prevenir os ataques cibernéticos em empresas.

Portanto, a legislação brasileira pode auxiliar a prevenir ataques cibernéticos a empresas e pessoas físicas através de dispositivos normativos que tratam sobre a punição dos sujeitos ativos dos crimes cibernéticos (Lei Carolina Dieckmann, Lei nº 14.155/2021 e Código Penal), do estabelecimento de parâmetros para o uso da

Internet no Brasil (Marco Civil da Internet) e das sanções administrativas pelo descumprimento da Lei Geral de Proteção de Dados Pessoais.

10 REFERÊNCIAS

ABREU, Cristiano Nabuco de; EISENSTEIN, Evelyn; ESTEFENON, Susana Graciela B. (org.) **Vivendo Esse Mundo Digital:** impactos na saúde, na educação e nos comportamentos sociais. Porto Alegre: Artmed, 2013.

AGRA, Andressa Dellay; BARBOZA, Fabrício Felipe Meleto. **Segurança de sistemas da informação**. Porto Alegre: SAGAH, 2018.

Agravamento dos crimes cometidos de forma eletrônica ou pela internet e competência em modalidades de estelionato: Lei nº 14.155/2021. Tribunal de Justiça do Estado de São Paulo. Disponível em: https://www.tjsp.jus.br/Download/SecaoDireitoCriminal/Cadicrim/AgravamentoCrimesInternet.pdf. Acesso em: 08 mar. 2023.

A importância do Brasil em aderir à convenção sobre o crime cibernético. Estadão. Disponível em:https://www.estadao.com.br/politica/blog-do-fausto-macedo/a-importancia-do-brasil-em-aderir-a-convencao-sobre-o-crime-cibernetico/#:~:text=A%20Conven%C3%A7%C3%A3o%20confere%20%C3%A0%20legisla%C3%A7%C3%A3o,Brasil%20em%20cumprir%20com%20a

Ainda há revelações a serem feitas sobre o Brasil". Consultor Jurídico. Disponível em:https://www.conjur.com.br/2014-jun-13/edward-snowden-ainda-revelacoes-serem-feitas-brasil. Acesso em: 08 mar. 2023.

ANPD publica regulamento de aplicação de sanções administrativas: Publicada, hoje (27/02), a Resolução da ANPD que permite à Autoridade aplicar punições por descumprimento à Lei Geral de Proteção de Dados (LGPD). Gov.br. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria. Acesso em 08 mar. 2023.

Aprovada adesão do Brasil à Convenção sobre o Crime Cibernético. Senado Notícias. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico. Acesso em: 08 mar. 2023.

Ataque DDoS – O que é e como se proteger. BHS. Disponível em: https://www.bhs.com.br/2023/01/11/ataque-ddos-o-que-e-e-como-se-proteger/. Acesso em: 08 mar. 2023.

Ataques de ransomwares podem provocar fechamento de mais de 30% dos negócios em alguns países. Forbes. Disponível em: https://forbes.com.br/forbes-tech/2021/07/ataques-de-ransomwares-podem-provocar-fechamento-de-mais-de-30-dos-negocios-em-alguns-paises/. Acesso em: 08 mar. 2023.

BELCIC, Ivan. **O que é uma botnet?.** Avast. Disponível em: https://www.avast.com/pt-br/c-botnet. Acesso em: 08 mar. 2023.

BIONI, Bruno. (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

BOTELHO, Vinicius. **Falsa sensação de impunidade nas redes sociais não isenta de culpa responsáveis por crimes.** Jornal da USP. Acesso em: https://jornal.usp.br/atualidades/falsa-sensacao-de-impunidade-nas-redes-sociais-nao-isenta-de-culpa-responsaveis-por-crimes/. Disponível em: 08 mar. 2023.

BRASIL. **Decreto-Lei Nº 3.914, de 9 de dezembro de 1941.** Lei de introdução do Código Penal (decreto-lei n. 2.848, de 7-12-940) e da Lei das Contravenções Penais (decreto-lei n. 3.688, de 3 outubro de 1941). Acesso em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3914.htm. Disponível em: 08 de mar. 2023.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08 mar. 2023.

_____. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 08 mar. 2023.

_____. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em:https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 08 mar. 2023.

_____. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 08 mar. 2023.

_____. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais. Acesso em: 08 de mar. 2023.

_____. **Decreto Legislativo Nº 37, de 2021.** Disponível em: https://www2.camara.leg.br/legin/fed/decleg/2021/decretolegislativo-37-16-dezembro-2021-792105-publicacaooriginal-164114-pl.html. Acesso em 08 mar. 2023.

_____. **Lei 14.155, de 27 de maio de 2021.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 08 mar. 2023.

_____. **Resolução CD/ANPD Nº 4, de 24 de fevereiro de 2023.** Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em: 08 mar. 2023.

_____. **Lei Nº 7.347, de 24 de julho de 1985**. Disciplina a ação civil pública de responsabilidade por danos causados ao meio-ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico e paisagístico (VETADO) e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm. Acesso em: 08 mar. 2023.

_____. **Lei nº 9.008, de 21 de março de 1995.** Cria, na estrutura organizacional do Ministério da Justiça, o Conselho Federal de que trata o art. 13 da Lei nº 7.347, de 24 de julho de 1985, altera os arts. 4º, 39, 82, 91 e 98 da Lei nº 8.078, de 11 de setembro de 1990, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9008.htm#:~:text=LEI%20N%C2%BA%209.008%2C%20DE%2021%20DE%20MAR%C3%87O%20DE%201995.&text=Cria%2C%20na%20estrutura%20organizacional%20do,1990%2C%20e%20d%C3%A1%20outras%20provid%C3%AAncias. Acesso em: 08 mar. 2023.

_____. 27ª Câmara de Direito Privado. **Apelação Cível 1000331-24.2021.8.26.0003.** TJSP. Apelante: Dorival Lasincki. Apelado: Eletropaulo Metropolitana Eletricidade de São Paulo S/A. Relator: Alfredo Attié. Data de Julgamento: 16/11/2021. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=15191761&cdForo=0. Acesso em: 08 mar. 2023.

_____. 2ª Turma Cível. **Agravo de Instrumento 0749765-29.2020.8.07.0000**.TJDFT. Agravante: Ministério Público do Distrito Federal e dos Territórios. Agravado: Serasa S.A. Relator: Cesar Loyola. Data de Julgamento: 26/05/2021. Disponível em: https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj. Acesso em: 08 mar. 2023.

Brasil aprova adesão à Convenção de Budapeste que facilita cooperação internacional para combate ao cibercrime. Ministério Público Federal. Disponível em: https://www.mpf.mp.br/pgr/noticias-pgr/brasil-aprova-adesao-a-convencao-de-budapeste-que-facilita-cooperacao-internacional-para-combate-ao-cibercrime. Acesso em: 08 mar. 2023.

Brasil é o 5º maior alvo de crimes cibernéticos. Época Negócios. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2021/09/brasil-e-o-5-maior-alvo-de-crimes-ciberneticos.html. Acesso em: 08 mar. 2023.

BRANDÃO, Emerson. **Roubo e vazamento de dados lideram ciberataques no Brasil, aponta IBM.** Uol. Disponível em: https://gizmodo.uol.com.br/roubo-e-vazamento-de-dados-lideram-ciberataques-no-brasil-aponta-ibm/. Acesso em: 08 mar. 2023.

BRITO, Auriney. **Direito penal informático**. São Paulo: Saraiva, 2013.

BROOKSHEAR, J. Glenn. **Ciência da computação:** uma visão abrangente. Tradução de Eduardo Kessler Piveta. 11. ed. Porto Alegre: Bookman, 2013.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. 1ª ed. Rio de Janeiro: Brasport, 2014.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

CARVALHO, André C. P. L. F de; LORENA, Ana Carolina. **Introdução à computação:** hardware, software e dados. 1. ed. Rio de Janeiro: LTC, 2017.

Conselho da Europa. Direção-Geral do ensino Superior. Disponível em: https://www.dges.gov.pt/pt/pagina/conselho-da-europa. Acesso em: 08 mar. 2023.

Convenção de Budapeste é promulgada sob a forma do Decreto Legislativo Nº 37. Opice Blum. Disponível em: https://opiceblum.com.br/convencao-de-budapeste-e-promulgada-sob-a-forma-do-decreto-legislativo-no-37/. Acesso em: 08 mar. 2023.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

_____. **Por que é mais difícil mentir hoje em dia**. Linkedin. Acesso em: https://pt.linkedin.com/pulse/por-que-%C3%A9-mais-dif%C3%ADcil-mentir-hoje-em-dia-crespo-ph-d-ccep-i. Disponível em: 08 mar. 2023.

DALE, Nell; LEWIS, John. **Ciência da Computação**. Tradução de Jorge Duarte Pires Valério. Rio de Janeiro: LTC, 2010.

Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. G1. Disponível em:https://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. Acesso em: 08 mar. 2023.

Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. G1. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml?utm_source=share-universal&utm_medium=share-bar-app&utm_campaign=materias. Acesso em: 08 mar. 2023.

Estados-Membros. Council of Europe. Disponível em: https://www.coe.int/pt/web/about-us/our-member-states. Acesso em: 08 mar. 2023.

Facebook é condenado a pagar R$ 6,6 mi por vazar dados de usuários. Gov.br. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/facebook-e-condenado-a-pagar-r-6-6-mi-por-vazar-dados-de-usuarios#:~:text=Bras%C3%ADlia%2C%2023%2F08%2F2022,de%20dados%20de%20usu%C3%A1rios%20brasileiros. Acesso em: 08 mar. 2023.

FEDELI, Ricardo Daniel; POLLONI, Enrico Giulio Franco; PERES, Fernando Eduardo. **Introdução à ciência da computação**. 2. ed. São Paulo: Cengage Learning, 2010.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital e a sociedade da informação.** 2. ed. São Paulo: Saraiva, 2016.

FREIRE, Emerson; BATISTA, Sueli Soares dos Santos. **Sociedade e Tecnologia na Era Digita**l. 1ª ed. São Paulo: Érica, 2014.

GARCIA, Lara R. et al. **Lei Geral de Proteção de Dados (LGPD)**: Guia de implantação. São Paulo: Blucher, 2020.

GOGONI, Ronaldo. **Deep Web e Dark Web: qual a diferença?.** Tecnoblog. Acesso em: https://tecnoblog.net/responde/deep-web-e-dark-web-qual-a-diferenca/. Disponível em: 08 mar. 2023.

GRECO, Rogério. **Curso de direito penal:** volume 1: parte geral: arts. 1º a 120 do Código Penal. 24. ed. Barueri (SP): Atlas, 2022.

GUIMARÃES, Fernanda. GONSALVES, Wesley. **Tentativas de ataque hacker atingem uma empresa a cada segundo no País.** Estadão. Disponível em: https://www.estadao.com.br/economia/negocios/ciberataques-hacker-ransomware-empresas-brasil/#:~:text=O%20c%C3%A1lculo%2C%20de%20um%20estudo,uma%20tentativa%20de%20ataque%20hacker. Acesso em: 08 mar. 2023.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital:** transformação digital: desafios para o direito. 2. ed. Rio de Janeiro: Forense, 2022.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

Lei Carolina Dieckmann: 10 anos da lei que protege a privacidade dos brasileiros no ambiente virtual. Defensoria Pública Geral do Estado do Ceará. Disponível em: https://www.defensoria.ce.def.br/noticia/lei-carolina-dieckmann-10-anos-da-lei-que-protege-a-privacidade-dos-brasileiros-no-ambiente-virtual/. Acesso em: 08 mar. 2023.

LEITE, George Salomão; LEMOS, Ronaldo. (coord.) **Marco Civil da Internet**. São Paulo: Atlas, 2014.

LENZA, Pedro. **Direito Constitucional**. 26. ed. São Paulo: SaraivaJur, 2022. (Coleção Esquematizado®)

LGPD - Lei Geral de Proteção de Dados. Conselho da Justiça Federal. Disponível em: https://www.cjf.jus.br/publico/lgpd/index.html. Acesso em: 08 mar. 2023.

MACHADO, Felipe Nery Rodrigues. **Segurança da Informação**: princípios e controle de ameaças. 1 ed. São Paulo: Érica, 2014.

MARTINI, Renato. **Sociedade da informação:** para onde vamos. 1ª ed. São Paulo: Trevisan Editora, 2017.

MORAES, Alexandre de. **Direito Constitucional**. 38. ed. Barueri (SP): Atlas, 2022.

MOTTA, Sylvio. **Direito Constitucional:** teoria, jurisprudência e questões. 29 ed. Rio de Janeiro: Forense; MÉTODO, 2021.

Mundo se aproxima da marca de 5 bilhões de usuários de internet, 63% da população. Insper. Disponível em: https://www.insper.edu.br/noticias/mundo-se-aproxima-da-marca-de-5-bilhoes-de-usuarios-de-internet-63-da-populacao/. Acesso em: 08 mar. 2023.

Nova Lei de crimes cibernéticos entra em vigor. Ministério Público do Estado de São Paulo. Disponível em: http://www.mpsp.mp.br/portal/page/portal/cao_criminal/notas_tecnicas/NOVA%20LEI%20DE%20CRIMES%20CIBERN%C3%89TICOS%20ENTRA%20EM%20VIGOR.pdf. Acesso em: 08 mar. 2023.

NUCCI, Guilherme de Souza. **Curso de direito penal:** parte geral: arts. 1º a 120 do Código Penal. 6. ed. Rio de Janeiro: Forense, 2022.

PADILHA, Rodrigo. **Direito Constitucional.** 6 ed. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2020.

Painel LGPD nos Tribunais: Jurisprudência do 2º ano de vigência a Lei Geral de Proteção de Dados. Disponível em: https://painel.jusbrasil.com.br/#Conclusoes. Acesso em: 08 mar. 2023.

PALFREY, John; GASSER, Urs. **Nascidos na era digital:** entendendo a primeira geração de nativos digitais. Tradução de Magda França Lopes. Porto Alegre: Artmed, 2011.

PINHEIRO, Patricia Peck. **Direito Digital**. 7 ed. São Paulo: Saraiva Educação, 2021.

_____. **Proteção de dados pessoais: comentários à Lei N. 13.709/2018 (LGPD)**. 3. ed. São Paulo: Saraiva, 2021.

_____(org.). **Segurança digital:** proteção de dados nas empresas. São Paulo: Atlas, 2021.

Promulgada PEC que inclui a proteção de dados pessoais entre direitos fundamentais do cidadão. Câmara dos Deputados. Disponível em: https://www.camara.leg.br/noticias/850028-promulgada-pec-que-inclui-a-protecao-de-dados-pessoais-entre-direitos-fundamentais-do-cidadao/. Acesso em: 08 mar. 2023.

Proteção de Dados Pessoais agora é um direito fundamental: Promulgada hoje, a Emenda Constitucional 115/2022 elenca a proteção de dados pessoais como

garantia fundamental. Gov.br. Disponível em: https://www.gov.br/anpd/pt-br/protecao-de-dados-pessoais-agora-e-um-direito-fundamental. Acesso em: 08 mar. 2023.

ROCHA, Johnny. **Lei Carolina Dieckmann completa 10 anos com baixa efetividade, avalia especialista**: Para presidente do Instituto de Proteção das Garantias Individuais, leis precisam acompanhar ritmo do avanço das tecnologias. Jota. Disponível em: https://www.jota.info/justica/lei-carolina-dieckmann-completa-10-anos-com-baixa-efetividade-avalia-especialista-02122022. Acesso em: 08 mar. 2023.

Saiba mais sobre o ex-agente que vazou dados de segurança dos EUA. G1. Disponível em:https://g1.globo.com/mundo/noticia/2013/06/patriota-ou-traidor-snowden-agiu-por-medo-da-intrusao-governamental-2.html. Acesso em: 08 mar. 2023.

SANTOS, Milton. **Por Uma Outra Globalização:** do pensamento único à consciência universal. Rio de Janeiro: Record, 2006.

SCHWAB, Klaus. **A Quarta Revolução Industrial.** Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SILVA, Leonardo Werner. **Internet foi criada em 1969 com o nome de "Arpanet" nos EUA.** Folha de S.Paulo. Disponível em: https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml#:~:text=A%20Arpanet%20era%20uma%20garantia,se%20maior%20no%20%C3%A2mbito%20acad%C3%AAmico. . Acesso em: 08 mar. 2023.

SILVA, Louise S. H. Thomaz da; SOUTO, Fernanda R.; OLIVEIRA, Karoline F.; et al. **Direito Digital**. Porto Alegre: SAGAH, 2021.

SOARES, Nycolle. **28 principais casos de vazamentos de dados da história**. Lara Martins Advogados. Disponível em: https://laramartinsadvogados.com.br/artigos/28-principais-casos-de-vazamentos-de-dados-na-historia/. Acesso em: 08 mar. 2022.

SUZUMURA, Daniel. **Estudo IBM: Roubo de dados lidera ataques cibernéticos no Brasil.** Jornal Dia Dia. Disponível em: https://jornaldiadia.com.br/estudo-ibm-roubo-de-dados-lidera-ataques-ciberneticos-no-brasil/. Acesso em: 08 mar. 2023.

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. 2 ed. São Paulo: Saraiva, 2015.

TAVARES, Tarcísio Alves. **Análises iniciais e críticas à Lei 12.737/2012 - Lei Carolina Dieckmann.** Orientador: Colimar Dias Braga Júnior. 2013. 11 f. Universidade Presidente Antônio Carlos - UNIPAC, 2013. Disponível em: https://ri.unipac.br/repositorio/wpcontent/uploads/2019/08/TARC%C3%8DSIO-ALVES-TAVARES.pdf. Acesso em: 08 mar. 2023.

TAKAHASHI, Tadao (org.). **Sociedade da informação no Brasil:** livro verde. Brasília: Ministério da Ciência e da Tecnologia, 2000.

TEIXEIRA, Tarcisio. **Direito Digital e Processo Eletrônico**. 6. ed. São Paulo: SaraivaJur, 2022.

TEIXEIRA, Tarcisio; GUERREIRO, Ruth Maria. **Lei Geral de Proteção de Dados Pessoais:** comentada artigo por artigo. 4. ed. São Paulo: SaraivaJur, 2022.

Vazamentos de dados provocados por ataques cibernéticos colocam reputação das empresas em risco. Valor Econômico. Disponível em: https://valor.globo.com/patrocinado/microsoft/ciber-seguranca/noticia/2022/05/19/vazamentos-de-dados-provocados-por-ataques-ciberneticos-colocam-reputacao-das-empresas-em-risco.ghtml. Acesso em: 08 mar. 2023.